Program Research Project

# REFLECTIONS ON A STRATEGIC VISION FOR COMPUTER NETWORK OPERATIONS

BY

COLONEL JOHN R. MAHONEY
United States Marine Corps Reserve



USAWC CLASS OF 2010



U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From - To)* |
|---|---|---|
| 25-05-2010 | Program Research Project | 01-11-2009 – 12-05-2010 |

**4. TITLE AND SUBTITLE**

Reflections on a Strategic Vision for Computer Network Operations

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

COL John R. Mahoney

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

COL Alan M. Phaneuf
Department of Distance Education

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Distribution A: Unlimited

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

US Geographic Combatant Commands (GCC's) are unprepared to effectively plan computer network operations (CNO) and incorporate them into military operations. This condition is not due to any failure of GCC commanders to recognize their warfighting responsibility. Current legal authorities and national policy primarily enable CNO support at the strategic level of war. However, they marginalize GCC CNO planning efforts by denying commanders CNO decision-making authority in the more decisive operational cyberwar. This paper will discuss the efficacy of this current approach to CNO within a framework of its missing component: a Department of Defense (DoD) strategic vision for how to use CNO to help win wars in the cyberspace domain.

**15. SUBJECT TERMS** Computer network operations, CNO, computer network attack, CNA, computer network attack – operational preparation of the environment, CNA-OPE, computer network defense, CND, computer network defense – response actions, CND-RA, computer network exploitation, CNE, Basic Computer Network Operations Planners Course, BCNOPC, cyberspace, Cyber, Cyberspace Operations, Cyber-Intelligence, National Military Strategy for Cyberspace Operations, NMSCO, Information Operations, IO

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | **19b. TELEPHONE NUMBER** *(include area code)* |
| UNCLASSIFED | UNCLASSIFED | UNCLASSIFED | UNLIMITED | 30 | |

USAWC PROGRAM RESEARCH PROJECT

# REFLECTIONS ON A STRATEGIC VISION FOR COMPUTER NETWORK OPERATIONS

by

Colonel John R. Mahoney
United States Marine Corps Reserve

Topic Approved By
Colonel Alan M. Phanuef

This PRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

## ABSTRACT

AUTHOR: Colonel John R. Mahoney

TITLE: Reflections on a Strategic Vision for Computer Network Operations

FORMAT: Program Research Project

DATE: 25 May 2010 WORD COUNT: 5,500 PAGES: 30

KEY TERMS: Computer Network Operations, CNO, Computer Network Attack, CNA, Computer Network Attack – Operational Preparation Of The Environment, CNA-OPE, Computer Network Defense, CND, Computer Network Defense – Response Actions, CND-RA, Computer Network Exploitation, CNE, Basic Computer Network Operations Planners Course, BCNOPC, Cyberspace, Cyber, Cyberspace Operations, Cyber-Intelligence, National Military Strategy For Cyberspace Operations, NMSCO, Information Operations, IO

CLASSIFICATION: Unclassified

US Geographic Combatant Commands (GCC's) are unprepared to effectively plan computer network operations (CNO) and incorporate them into military operations. This condition is not due to any failure of GCC commanders to recognize their warfighting responsibility. Current legal authorities and national policy enable CNO primarily at the strategic level of war. They marginalize GCC CNO planning efforts by denying commanders CNO decision-making authority in the more decisive operational cyberwar. This paper will discuss the efficacy of this current approach to CNO within a framework of its missing component: a Department of Defense (DoD) strategic vision for how to use CNO to help win wars in the cyberspace domain.

# REFLECTIONS ON A STRATEGIC VISION FOR COMPUTER NETWORK OPERATIONS

Where there is no vision, the people perish.

—Proverbs 29:18[1]

US Geographic Combatant Commands (GCC's) are unprepared to effectively plan computer network operations (CNO) and incorporate them into military operations. This condition is not due to any failure of GCC commanders to recognize their warfighting responsibility. Current legal authorities and national policy enable CNO primarily at the strategic level of war. They marginalize GCC CNO planning efforts by denying commanders CNO decision-making authority in the more decisive operational cyberwar. This paper will discuss the efficacy of this current approach to CNO within a framework of its missing component: a Department of Defense (DoD) strategic vision for how to use CNO to help win wars in the cyberspace domain.

GCC's do not have sufficient authority to integrate CNO into their operational plans. The authority to procure computer network attack (CNA) capabilities (i.e, tools and weapons) is held by the Services.[2] GCC authority to conduct cyber attacks remains remarkably limited.[3] A Functional Combatant Command (FCC), USSTRATCOM, directs the overall operation and defense of the GCC's computer networks.[4] Additionally, the intelligence collection component of computer network exploitation (CNE) is a function of the intelligence community (IC). GCC's are unable to integrate CNO into their planning process because they do not sufficiently control any of the pillars of CNO.

An additional deficiency that exacerbates this situation is that DoD has no comprehensive CNO strategic vision; "that picture of future changes desired by governmental elites [that] takes into account the probabilities of informed extrapolations

of current foreign and domestic trend lines that will affect national security."[5] Strategic vision describes a realistic and compelling future orientation and provides a strategy to achieve it.[6] In today's existing cyberwar, the US has yet to conceptualize a way to win.

It is necessary to take an objective look at this current situation in order to begin creating a strategic vision for how DoD will plan CNO and fight successfully in cyberspace. This paper starts by examining the nature and object of war in cyberspace and the role that CNO plays in it. Next, it identifies key definitions and discusses their implications. It follows with an examination of relevant national strategic guidance, the DoD organizations bound by it, and trends in DoD cyberspace activities. This paper evaluates each of these in terms of its importance to developing a strategic vision. It then makes recommendations for a future CNO planning environment that better serves US national security interests.

Strategic versus Operational Cyberwar

"The first, the supreme, the most far-reaching act of judgment that the statesman and the commander have is to establish... the kind of war on which they are embarking."[7] This section examines cyberspace war (i.e., cyberwar), its relationship to physical war, and the use of CNO to cause effects at both the strategic and operational levels of war.

There are several unofficial definitions of cyberwar; however, there is currently no authoritative definition in joint doctrine.[8] A general description is that cyberwar is a composite of offensive, defensive, and enabling actions taken in and through the cyberspace domain to compel a state or non-state actor to do the will of an opponent actor.[9] DoD supports both strategic and operational cyberwar but is not currently well postured for the latter.

*Strategic Cyberwar*. By its nature, cyberwar is non-physical. It is a less dominant form of war than physical war. “It is almost inconceivable that a sufficiently vigorous cyberwar can overthrow the adversary’s government and replace it with a more pliable one.”[10] Strategic cyberwar *cannot* produce a decisive battle that determines the overall outcome of either a traditional or an irregular war. It *cannot* include the disarmament or destruction of enemy forces or the occupation of its geographic territory. Physical war, in contrast, *can* do these things. Cyberwar can cause significant disruptions, even very expensive ones, but it cannot cause a determined opponent to surrender.[11]

Strategic cyberwar must seek ends that are more limited than those of physical war. Its enabling assumption, therefore, is that all opponents agree to keep the war non-physical.[12] In a case where one adversary sufficiently denied another’s access to cyberspace, the victim would likely escalate to physical war before it would surrender its objective. Escalation to physical conflict, however, causes the nature of a cyberwar to shift from strategic cyberwar to operational cyberwar; one in which operations conducted in cyberspace play a supporting, rather than the dominant role in the overall war. The only realistic ends of strategic cyberwar, therefore, are to frustrate an opponent, exhaust that opponent’s resources and to deter escalation to physical war. The achievable ends of the current US strategic cyberwar against various global cyber threats must, for these reasons, be limited to cyber-deterrence and cyber-defense.

*Operational Cyberwar*. “Operational cyberwar consists of wartime cyber attacks against military targets and military-related civilian targets.”[13] Its enabling assumption, therefore, is that the proper use of cyber attack is to “support physical military operations.”[14] Like strategic cyberwar, “operational cyberwar cannot win an overall war

on its own."[15] Since GCC's plan and direct the execution of operational warfare, it follows that operational cyberwar is more appropriate for them than it is for the FCC (i.e., USSTRATCOM/USCYBERCOM) and the national intelligence agencies that are currently better resourced for its execution.

Unlike strategic cyberwar, operational cyberwar is potentially decisive.[16] It can achieve three basic objectives.[17] The first is to create a surprise cyber attack that can cripple a capability the enemy will rely on having at a specific time or for a specific event (e.g., a distributed denial of service cyber attack against a critical node in an opponent's Intelligence network). The second is to use a CNO capability as a tactical weapon in order to achieve a temporary, but potentially decisive advantage during an operational campaign (e.g., a cyber attack against a fire control network's human-machine interface (HMI)). The third, used sparingly, can disrupt an enemy's confidence in networked systems, causing shifts to less efficient forms of command and control (C2), propaganda, fundraising, recruiting and training (e.g., attacks to randomly redirect C2 emails and webpage access attempts).

*The Role of Intelligence in Cyberwar*. A primary challenge in cyberwar is to acquire a detailed understanding of the computer networks used by an enemy. More importantly, knowing how an enemy will react to failure of those networks is critical. This underscores the question of who should plan and execute a cyber attack: intelligence operatives or military operators. Intelligence operatives obtain detailed knowledge of enemy networks. Military operators, on the other hand, may better understand how a decision-maker would conduct operations without it. Martin Libicki of the RAND Corporation writes that "those best placed to plan a military campaign that uses

operational cyberwar... are more likely to be military operators rather than intelligence operatives."[18] Current US policies favor the intelligence community (IC), which enjoys the preponderance of skilled practitioners, equipment resources, and authorities.

*Expanding the US Focus to Include Operational Cyberwar*. Current US national strategic policy over-focuses on strategic cyberwar and marginalizes the potentially more decisive results that GCC's could achieve in operational cyberwar.[19] Authorities and policies empower national strategic organizations to conduct a strategic cyberwar that is best suited for cyber-defense and cyber-deterrence. There is no argument against continuing this vigilance but the goals of strategic cyberwar should no longer be so exclusive that they obfuscate the GCC's ability to conduct operational cyberwar. A strategic vision for CNO would guide decision-makers to realign appropriate legal authorities and cyber resources, and to assign trained personnel to the GCC's, empowering them to plan and conduct operational cyberwar.

Words have Meaning

A first step in drafting a strategic vision for CNO is to examine its often-confusing lexicon.

*Cyberspace.* Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[20] The significance of this definition is that it identifies cyberspace as a new warfighting *domain,* distinct from the land, air, maritime, and space domains. Domains are where warfighting occurs. War-*fighting* involves C2, fires, movement and maneuver, sustainment, protection, and intelligence functions.[21] GCC's

are the essential directors of these functions, linking “US national strategy and operational activities within a theater.”[22]

The ability to plan CNO is critical because effective operations in this domain are “the prerequisite to effective operations across all strategic and operational domains – securing freedom from attack and the freedom to attack.”[23] Without the ability to plan effective CNO at the GCC’s, military operations in all other domains are at risk.

*Cyberspace Operations, Network Operations (NETOPS), and the Global Information Grid (GIG).* A term closely related to cyberspace is “cyberspace operations,” which is “the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include CNO and activities to operate and defend the Global Information Grid (GIG).”[24] This definition implies that “cyberspace operations” consists of at least two distinct activities, CNO and “activities to operate and defend the GIG.”

The definition of network operations (NETOPS) is “activities conducted to operate and defend the GIG.”[25] Therefore, cyberspace operations include a combination of CNO and NETOPS.

The GIG is “the globally interconnected, end-to-end set of information capabilities, associated processes and personnel for acquiring, processing, storing, transporting, controlling, and presenting information on demand to joint fires and support personnel.”[26] Since the infrastructure defined here is o*n demand to joint fires and support personnel*, reference to the GIG means the DoD portion of the internet.

*Computer Network Operations (CNO).* The definition of CNO is somewhat vague. It is “comprised of computer network attack (CNA), computer network defense

(CND), and related computer network exploitation (CNE) enabling operations." [27] Notably, this definition does not tell the reader what CNO is, only what comprises it.

This definition of CNO implies that "CNA, CND, and related CNE enabling operations" are different activities. The implication from the definition of "cyberspace operations" is that CNO is an "operation" to achieve objectives that contribute to the "employment of cyber capabilities" in or through cyberspace. It then follows that CNO is essentially a planning function that results in some integrated, coordinated, and synchronized operation that is a combination of actions associated with CNA, CND, and related CNE enabling operations.

*Computer Network Exploitation (CNE)*. The definition of CNE is "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[28] This implies that CNE has two sub-elements, one that is an operations activity (the "enabling operations"), and another that is an intelligence function ("collection"). At issue is whether it is only the IC that conducts CNE (under its Title 50 authority), or if there is a complementary role for the operations community to perform in the enabling operations function (under its Title 10 authority).

This issue is important for the operations community. The definition of CNO does *not* include the intelligence sub-element of CNE since it is simply "comprised of CNA, CND, and *related CNE enabling operations*"[29] [italics added]. Devoid of the intelligence collection sub-element of CNE, CNO remains an operational function. In doctrine, therefore, CNO is comprised of CNA, CND, and just one of the two sub-elements of CNE.

*Computer Network Attack (CNA).* CNA is "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[30] CNA is an offensive activity. As such, the authority to conduct a CNA belongs to the operations community. The IC, however, plays a significant role in preparing military operators to execute CNA. Its role involves conducting CNE and providing related intelligence support to the operations community in order for an attack to be effective.

Current policy correctly assigns responsibility for operational maneuver to GCC commanders but, unfortunately, reserves much of the authority to execute supporting CNA to USSTRATCOM. The first issue of concern with this policy is that it conditions the IC to deal more directly with an FCC than it does with the supported GCC. The second issue is that this policy complicates GCC efforts to conduct CNO planning.

In order to achieve the defensive and deterrent ends of the strategic cyberwar, it is appropriate that the IC maintain its close supporting relationship with USSTRATCOM. In fighting the neglected operational cyberwar, though, the IC must support the GCC's in a similarly direct and timely manner. A strategic vision should propose an equally close supporting relationship between the IC and the GCC's. Without it, CNO planning is further complicated due to reduced intelligence timeliness and insufficient network intelligence detail provided to the GCC's planning staff.

*CNA-Operational Preparation of the Environment (CNA-OPE).* CNA-OPE is an operational authority related to the authority to conduct CNA. CNA-OPE is "operations conducted to gain and/or confirm access to, and gather key information on the targeted network concerning the capabilities and configuration of, targeted networks or systems

and to facilitate target acquisition and target analysis in preparation for CNA and/or other offensive missions."[31] This is the authority to use cyberspace tools to gain access to targeted computers and computer networks in order to determine their continued relevance and confirm attack parameters, as long as its intent is not the collection of intelligence. A GCC can consider CNA-OPE to be similar to the "related CNE enabling operations" discussed in the CNO definition section above.

A pre-requisite for the GCC to execute CNA-OPE is that IC must first provide an initial description of the key network links and nodes against which the attack will occur. The GCC commander can then better conduct CNA-OPE in order to ensure access and validate attack parameters before executing a successful CNA. A strategic vision for CNO should emphasize this GCC requirement.

*Computer Network Defense (CND).* CND is defined as "actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks."[32]

There is often confusion about the difference between CND and the "defend" role identified in the definition of NETOPS. In theory, the difference is that CND considers the potential impact of cyber threats from *outside* the network. NETOPS considers the reliability and efficiency of the network that can be achieved by "hardening" it from the *inside*. As a practical matter, the personnel with CND expertise are the same individuals that do NETOPS; the information technology (IT) professionals normally assigned to the Communications (G/S-6) section and similar, specialized organizations. CND and NETOPS, therefore, have an overlapping relationship. NETOPS professionals

conduct CND while CNO planners integrate CND activities with CNA, CNE, and other related actions in support of the commander's overall mission objectives.

*Computer Network Defense – Response Actions (CND-RA).* An authority closely related to CND is CND-RA. It is "deliberate, authorized defensive measures or activities that protect and defend DoD computer systems and networks *under attack or targeted for attack* [italics added] by adversary computer systems/networks."[33] There are several increasingly aggressive levels of CND-RA.

While at its most aggressive level[34] there are similarities between CND-RA and CNA, a CND-RA is aggressive but not offensive. It is a defensive act, not an attack, executed to prevent an ongoing or anticipated attack against the friendly network from being more effective than it would be without an aggressive response.

In practice, CNO is a planning function that integrates, coordinates, and synchronizes the five activities identified above: CNA, CNA-OPE, CND, CND-RA, and CNE. The CNO planner performs none of these activities. The planner's job is to communicate with the individuals, organizations, and agencies that execute the activities and coordinate for their conduct to support the military objectives articulated by the commander.

To support the requirements of the strategic cyberwar, current national policies retain most authorities and resources for the execution of the five activities at national strategic organizations and agencies. This has a detrimental effect on GCC's because it negatively affects their ability to plan and execute CNO in support of the operational cyberwar. The following section includes a more detailed examination of these national policies.

National Strategic Direction

Much of the guidance published about cyberspace operations and CNO is classified. This section is, therefore, limited in its scope by the guidance available at the unclassified level. A strategic vision should evaluate the necessity of maintaining so much of the relevant discussion at the classified level. Perhaps the broader operations community could provide better insights once it is more widely informed from new unclassified literature and discussion.

*National Security Strategy of the United States of America (NSS)*. The NSS, signed by the President, declares that DoD is "pursuing a future force that will provide tailored deterrence of... threats (including ... terrorist attacks in the ... information domain)."[35] It is not hard to see this seminal guidance reflected in the national focus on cyber-deterrence and its emphasis on the strategic level of cyberwar. The document does not address CNO specifically but it does reveal the strategic direction in which the DoD is to move.

The NSS recognizes that DoD "is transforming itself to better balance its capabilities [against]... disruptive challenges from... actors who employ technologies and capabilities (such as... cyber operations)."[36] This guidance encourages a military transformation within DoD and specifies the need for "a better balance" in its approach to cyberspace operations. A strategic vision for CNO, therefore, should provide an achievable future orientation on how the military can support *both* the strategic and the operational cyberwar.

*National Strategy to Secure Cyberspace (NSSC)*.[37] The NSSC provides overarching policy guidance regarding the nation's *defensive* approach to cyber security. It identifies several national critical infrastructures and the lead government

agencies that are responsible for their cyber security. The NSSC also identifies the top five national cyber security priorities in terms of needed plans or programs.

This document calls for transparency and collaboration among all sectors of the US government and private sector. Even though more recently published cyber security guidance is discussed below, none of it supersedes or rescinds the NSSC. It continues to inform all subordinate NETOPS and CND planning and operations.

*Comprehensive National Cyber-security Initiative (CNCI)*. "Rather than serving as an overarching national strategy document with specific instructions for federal agency implementation..., the CNCI is seen as a plan of action for programs and initiatives."[38] It identifies several objectives that support its goal of comprehensively addressing the nation's cyber security concerns. Each is consistent with the national priorities described by the NSSC and, in this sense, is a natural extension of that document. It serves as a key roadmap for the roles of government and private activities at the strategic cyberwar level. It does not address the GCC's role specifically so its significance is limited as a guide to commanders planning military activities in the operational cyberwar.

*Cyberspace Policy Review (CPR, also known as "The 60-day Review").* Conducted shortly after President Obama took office, the CPR emphasizes the need for the nation to take immediate action to secure cyber-space. It provides both near- and mid-term action plans to assure "a trusted and resilient information and communications infrastructure."[39] President Obama approved the recommendations of the CPR in May 2009, establishing them as national strategic guidance. The CPR's focus is also at the

strategic cyberwar level and thus provides little guidance to GCC's regarding the conduct of CNO.

*The Unified Command Plan (UCP).* The UCP, signed by the President, "establishes the missions and geographic responsibilities among the [ten Unified] Combatant Commands."[40] It assigns significant responsibilities to the Commander, USSTRATCOM, for cyberspace operations.[41] The UCP also establishes the centrality of USSTRATCOM in the processes through which GCC's conduct cyber operations in both the strategic and operational cyberwars.

It serves as a principal source of guidance for CNO planning. The UCP establishes a central role for USSTRATCOM but, by requiring coordinated cyberspace operations with the GCC's, implies that the GCC's have CNO authorities apart from USSTRATCOM. It creates advantages for USSTRATCOM that include more efficient C2, improved unity of command, and a degree of standardization. A strategic vision might recommend UCP changes that specify the cyber missions and responsibilities of the GCC's.

*The National Military Strategy for Cyberspace Operations (NMS-CO).* An unclassified, publically available version of the NMS-CO offers guidance that supports this paper's thesis; that the ability to plan and conduct CNO should not be limited primarily to national-strategic organizations. Subordinate echelons can achieve decisive results if given appropriate authorities and CNO capabilities.

The NMS-CO declares, "operations to achieve desired effects in and through cyberspace require integration of organizations, capabilities, functions, technologies, and mission."[42] It is also specific about the responsibility of military leaders. First, it

directs that “senior leaders must establish a structure that integrates all mission areas and dismantles stove-piped organizations that hinder collaboration and lengthen decision-making cycles.”[43] It guides more than just the responsibility of senior leaders. The NMS-CO warns that the DoD will also “hold leaders at all levels responsible and accountable for cyberspace operations in the same manner as accountability is addressed in the other domains.”[44]

The current practice of maintaining most CNA authorities and capabilities at national strategic organizations is inconsistent with the NMS-CO. The document advises senior military leaders to “integrate capabilities across the full range of military operations using cyberspace [and] conduct collaborative planning for integrated cyberspace operations synchronizing with other military and intelligence operations.”[45] It even tells commanders how to do this. “C2 in cyberspace operations is achieving unified action vertically and horizontally, among all levels of war, and throughout organizations.”[46]

The NMS-CO shows that Defense Department policy favors a decentralized, cross-echelon distribution of CNO authorities, capabilities, and planning responsibilities. The practice of executing a national policy, which stresses interagency coordination due to its focus on strategic cyber defense and cyber deterrence, fails to loosen the reigns of centralization that impede the effective conduct of the operational cyberwar by the GCC’s. A strategic vision for CNO planning might emphasize a need to restructure organizations, C2, training, and the allocation of cyber resources.

*Doctrinal Guidance*. As late as February 2010, there were 78 currently approved joint doctrine publications.[47] Issues pertaining to cyberspace are a primary topic in only

two of them: Joint Publication (JP) 6-0, *Joint Communication Systems*, which discusses NETOPs[48] and CND;[49] and JP 3-13, Information Operations (IO), which describes CNO as a core capability of IO.[50] Although a new classified publication, JTP 3-12, *Cyberspace Operations*, is currently under development, these two unclassified publications do not adequately address specific CNO training requirements or the details of the CNO planning process. A strategic vision for CNO would propose the development of a more robust doctrinal library.

Organizational Trends

This section seeks to evaluate existing conditions, extrapolate emerging trends, and identify the underlying motivations in some of today's key cyberspace-related decisions. Three important trends are developing today that could transform the CNO community within the next five to fifteen years. They are the creation of US Cyber Command (USCYBERCOM), sub-delegation of CNO authorities and capabilities, and the increasingly significant role of the IC, specifically the Signals Intelligence (SIGINT) community, in the execution of not just CNE, but of CNO in general.

*US Cyber Command (USCYBERCOM)*. This new sub-unified command is a subordinate organization under USSTRATCOM. In the past, USSTRATCOM has sub-delegated CND missions to Joint Task Force – Global Network Operations (JTF-GNO). Concomitantly, it has sub-delegated CNA missions to Joint Functional Component Command – Network Warfare (JFCC-NW). The commander of JFCC-NW has also been "dual-hatted"[51] with the Director of the National Security Agency (DirNSA). DirNSA directs a Title 50 intelligence agency with the authority to conduct CNE, although USSTRATCOM has no authority over DirNSA in the execution of its Title 50 responsibilities.

In 2008, USSTRATCOM transferred operational control (OPCON) of JTF-GNO to JFCC-NW. For the first time, one three-star General held authorities for all the CNO components (i.e., CNA, CND, and CNE). The observed trend is an evolving consolidation of organizations that exercise authority for CNA (i.e., JFCC-NW), CND (i.e., JTF-GNO), and NSA (i.e., CNE).

In June 2009, SECDEF approved the establishment of USCYBERCOM, which will combine and then disestablish JTF-GNO and JFCC-NW. Its commander was the same three-star JFCC-NW commander, still dual-hatted as DirNSA. In May 2010, Congress approved promotion for the commander of USCYBERCOM (and of DirNSA), creating a new four-star, Title 10 commander of USCYBERCOM who will have legal authority for CNA, CND, and (under his Title 50 authority as DirNSA) CNE.

Although speculative, the President may eventually break USCYBERCOM out from under USSTRATCOM, establishing it as a separate unified command. If this occurs, one independent FCC uniquely configured to support cyberspace missions could significantly improve DoD CNO support to the various government and private sector cyber-security communities engaged in the strategic cyberwar. The major potential downside would be if increasing support requirements for the strategic cyberwar caused USCYBERCOM to decrease its integration and support to the GCC's, and thus further marginalize their CNO capabilities in the operational cyberwar.

*Sub-delegation of CNO Authorities and Capabilities.* GCC frustration with the often arduous and time-consuming Request and Approval (RAP) process for CNO support is growing. Both General Petraeus[52] and General Odierno[53] appealed to their superiors in Washington for more CNO support during their tenures as Commanding

General of Multi-National Forces Iraq (MNF-I). JFCC-NW recognized the need for this improved support in the operational cyberwar by establishing small, deployable teams of cyber experts to assist commanders and their CNO planning staffs.

In November 2009, the Army Training and Doctrine Command (TRADOC) released its draft "Cyberspace Operations Concept Capability Plan (CCP) for 2016 – 2028."[54] While this document frames of the problems within the Cyber, IO, and electronic warfare (EW) communities, it also offers a surprising vision that recognizes future cyber authorities and capabilities held *at the company and battalion* levels. Time will tell if it will be necessary to push CNO down to this level of tactical operations, but the document makes the trend clear. Eventually, the question from the operating forces will no longer be about what support the national community can provide. It will be about why the operating forces do not already have authorities and organic capability in place.

Graduate research at the Air Force Institute of Technology also examined three models (i.e., Independent, Interdependent, and Organic) for how USSTRATCOM [or USCYBERCOM] could accommodate this increasing demand for CNO support at lower command echelons.[55] A strategic vision might consider these three models as separate options or, alternatively, as a single process that starts with the first and matures into the second and third over time. For example, each GCC's Service Component Commands (SCC's) might initially establish a CNO proponent. Each GCC would next designate a cyberspace coordinating authority and USCYBERCOM would coordinate, integrate, and synchronize CNO planning and operations through them. As expertise and confidence grow, the Services could program more CNO personnel to support the GCC's through their SCC's. Eventually, the GCC's could establish subordinate CNO-

JTF organizations with augmentation from USCYBERCOM. Then, as these CNO-JTF's matured, they could become sub-unified commands under each GCC, greatly expanding the capacity of each for CNO planning and execution. The biggest drawback to this seems to be the willingness to commit resources to it and a strategic vision to guide the process.

*Expanding Role of the SIGINT Community*. Neither the CNA nor the CND communities can currently match the CNE (i.e., SIGINT) community in knowledge of the net or knowledge of the cyber threat. The operations community, which has authority to conduct CNA, CNA-OPE, CND, and CND-RA, is thoroughly dependent on the IC to provide detailed network intelligence in a timely manner. While USCYBERCOM and NSA are rectifying this challenge by consolidating capabilities into an operational command that the SIGINT community can support, they have not yet effectively addressed it for the benefit of the GCC's. Instead of expanding NSA support to the GCC's, the trend seems to be toward expanding the IC's activities into functions that are traditionally operational.

The EW community, for example, is becoming concerned that the convergence of electronic and computer technology may eventually result in their community becoming absorbed into the cyberspace community. The EW community, operating under Title 10 operational authorities, has enjoyed relatively simple execution authorities in the past. Once aligned with the CNO community, however, they are afraid that they will lose their flexibility to conduct operations. Additionally, SIGINT personnel employ many of the same technologies used by the EW community. The SIGINT community is large and well funded whereas the EW community is a relatively small

community which few senior leaders truly understand. The concern is that SIGINT personnel will eventually *execute* EW missions rather than simply support them.

The most telling sign of this trend, though, is that in the establishment of USCYBERCOM, the officer chosen to lead it was not from the operations community, but from the SIGINT community (i.e., DirNSA). This most significant CNO command assignment could have been a Title 10 operational commander (with authority for CNA and CND) who gained an expanded mission that included Title 50 CNE authority. Instead, an existing Title 50 commander (i.e., DirNSA) gained an expanded Title 10 mission. If USCYBERCOM is to better integrate CNO for the GCC's, a strategic vision should address whether an intelligence operative can achieve that goal better than if a military operator were in command.

Recommendations

This research has identified several issues that a strategic vision for CNO could address. The areas in which they find consensus with the views of other writers, commanders, planners, and practitioners could form the basis for a unifying strategic vision about CNO. The following are some initial recommendations for that vision.

First, national strategic leaders should immediately apportion to the GCC's appropriate legal authorities, cyber resources, and trained personnel, empowering them to organically plan and conduct operational cyberwar. The primary advantage of doing this is that it will enable the GCC's to directly plan and employ CNO capabilities in support of decisive operational actions that achieve overall strategic ends. The chief disadvantage is that it will decrease the overall capability of USCYBERCOM by redirecting some of the CNO resources programmed to support it. The chief risk is that by refocusing NSA and the IC on the GCC's, they will lose focus on the strategic

cyberwar. This is unlikely, though, since the Director of National Intelligence (DNI) and the President determine the national intelligence priorities.

Second, the SECDEF should develop and approve a plan to mature subordinate CNO JTF's at each GCC within the next year. The plan should direct each SCC supporting a GCC to establish a CNO proponent to coordinate with USCYBERCOM and NSA. Each GCC should establish a Cyberspace Coordinating Authority (CCA) to oversee all CNO proponent issues with the CNO stakeholder community. The plan should direct that the Services augment the SCC CNO proponents and GCC CCA's with trained CNO personnel. It should also establish the objective of maturing these organizations into a standing CNO JTF, with appropriate legal authorities and organic CNO capabilities, at each GCC within ten years. The great advantage of this is that it enables the warfighting commanders the ability to employ CNO decisively in support of operational maneuver when it is applicable. Its main disadvantages are that it requires significant personnel and other resources that the Services are not currently programmed to provide. The greatest risk, though, is having US operational forces face enemies who shape operations with a devastating cyber attack followed quickly with a vigorous physical one.[56]

Third, training programs that teach military CNO technical capabilities and planning skills should be significantly expanded throughout DoD. This should also include the development of doctrine, tactics, techniques, and procedures that are more extensive and kept at the unclassified level where possible. The advantage of this is that it will standardize both the lexicon and the processes for conducting CNO. The main disadvantage is that it will be difficult to gain wide consensus on the best

approach. Nonetheless, the risk of not choosing a reasonable end state that empowers the GCC's leaves US operational forces relatively unarmed for battle in the cyberspace domain.

Fourth, the next commander of USCYBERCOM should be a former GCC commander. This commander should also be dual-hatted as the DirNSA while an intelligence officer remains the Deputy DirNSA. The main advantage of this is that it will bring greater operational perspective to cyberspace operations and to the SIGINT community. Its chief disadvantage is that it will likely encounter extensive resistance from the IC. The risk, however, is that maintaining the focus of the IC on the strategic cyberwar at the expense of the operational cyberwar puts the successful accomplishment of both in jeopardy.

## Conclusion

This research indicates the national strategic community has focused on enabling a few key military organizations to support its fight in the strategic cyberwar. While this is well intentioned, it has not enabled the GCC's to succeed in the potentially more decisive operational cyberwar. Military adversaries that would challenge US strategic interests remain likely to engage GCC's in synchronized cyber and physical attacks at the operational level of war. It is time to empower the GCC's to fight them.

## Endnotes

[1] Bible.com Homepage, "King James Bible," http://bibleresources.bible.com/passagesearchresults2.php?passage1=Proverbs+29&book_id=24&version1=9&tp=31&c=29 (accessed 7 May 2010).

[2] For background on the requirements of the Military Departments to "develop and procure weapons, equipment, and supplies essential to the fulfillment of the functions assigned," see US Department of Defense, *Functions of the Department of Defense and its Major Components*,

Department of Defense Directive (DODD) 5100.1 (Washington, DC: Department of Defense, November 21, 2003), 13.

[3] (U//FOUO) For unclassified background on the role of the GCC's, see US Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: US Joint Chiefs of Staff, May 2, 2007 Incorporating Change 1 dated March 20, 2009), I-14. Generally, GCC authority is limited to the creation of effects contained within the geographic boundaries of the commander's area of responsibility (AOR). The global nature of cyberspace causes a concern that GCC-initiated CNA will cause trans-regional effects. For unclassified, official use only background on the role of combatant commanders to plan and conduct cyberspace operations, see George W. Bush, *The Unified Command Plan*, (Washington, DC: The White House, December 2008). The Unified Command Plan (UCP) assigns specific cyberspace authorities to USSTRATCOM, but the text only implies, rather than specifies, related authorities for GCC's.

[4] (U//FOUO) George W. Bush, *The Unified Command Plan*, (Washington, DC: The White House, December 2008), 11. While the UCP assigns authority to "direct Global Information Grid [GIG] operations and defense" to USSTRATCOM, this FCC has delegated the mission, as well as many of its other UCP cyberspace mission tasks, to USCYBERCOM. For more background about those delegated tasks, see US Strategic Command, *USCYBERCOM Announcement Message*, J3 Director of Global Operations Record Message DTG 212106Z May 2010 (Offutt AFB, NE: US Strategic Command, May 21, 2010).

[5] David Jablonsky, "Strategic Vision and Presidential Authority in the Post Cold-War Era," Parameters XXI, no. 4 (Winter 1991-92): 2.

[6] Glenda Y. Nogami, *What is This Thing called Strategic Vision?,* US Army War College paper presented at the International Military Testing Association Annual Convention in Rotterdam, The Netherlands, 1994 (Carlisle Barracks, PA: US Army War College, 1994), 4.

[7] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret, (Princeton, NJ: Princeton University Press, 1989), 608.

[8] US Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, (Washington, DC: US Joint Chiefs of Staff, 12 April 2001, as Amended Through 13 June 2007). There is no definition for "cyberspace war" or "cyberwar" in this authoritative DoD publication.

[9] A general description of cyberwar developed by the author.

[10] Martine C. Libicki, "Cyberdeterrence and Cyberwar,*" RAND Project Air Force,* (2009): 119.

[11] The 2007 cyber attack against the country of Estonia is an example of strategic level cyberwar that failed to be decisive. When the government of Estonia, a member of NATO, decided to move an historic statue that memorialized Soviet war dead to a less prominent location in its capital city, Russian patriots objected. Continued Estonian recalcitrance resulted in a massive distributed denial of service (DDOS) cyber attack against various government, financial, police, and emergency response websites. While not proven, these strategic level attacks presumably originated from within Russia and by Russian operatives around the world.

This campaign of cyber attacks did not have an accompanying Russian physical attack. Consequently, the Estonians continued to move the statue. For more information on this short cyberwar, see Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *New York Times*, May 29, 2007.

[12] Libicki, "Cyberdeterrence and Cyberwar," 122.

[13] Ibid., 139.

[14] Ibid., 117.

[15] Ibid., 140.

[16] The 2008 cyber attack against the country of Georgia is an example of operational cyberwar conducted in a manner supportive of a successful Russian physical attack against Georgian forces. South Ossetia, a relatively autonomous and demilitarized region of Georgia on the Georgian-Russian border, sought independence from Georgia. An independent South Ossetia served the strategic interests of Russia but not those of Georgia. As the Georgian government moved forces into South Ossetia to restore its territory, it experienced a significant campaign of cyber attacks, presumably of Russian origin. While this cyber attack was ongoing, Russian forces entered South Ossetia and moved against those of Georgia. Georgian forces were successfully defeated. For more background on this operational cyberwar in Georgia, see Eneken Tikk et al, *Cyber Attacks against Georgia: Legal Lessons Learned*, (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, November 2008).

[17] Ibid., 142.

[18] Ibid., 156. Libicki's argument that military operators are better suited to plan military operations is consistent with the premise underscoring a broader role for the GCC's in planning and executing CNO. Military operators are the most capable of creating the military advantages necessary to win battles. The IC is better suited to informing operational decision-makers about enemy capabilities and intentions.

[19] Ibid., Libicki, 6. Libicki writes, "operational cyberwar – cyber attacks to support warfighting, may have far greater purchase than strategic cyberwar – cyber attacks to affect state policy." This PRP addresses many of the national and strategic policy documents that describe the preponderant US focus on strategic cyber concerns. For a good reference on the current lack of similar emphasis at the operational and tactical levels, see Andre Abadie, *WWW.KASSERINEPASS.COM: Determining the US Army's Readiness for Tactical Operations in Cyberspace*, Master's Thesis, (Fort Leavenworth, KS: Army Command and General Staff College, December 6, 2009).

[20] Christopher J. Castelli, "Defense Department Adopts New Definition of Cyberspace," *Inside the Air Force*, 23 May 2008, http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm (accessed 1 May 2010).

[21] US Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, (Washington, DC: US Joint Chiefs of Staff, September 17, 2006 incorporating change 1 dated February 13, 2008), III-1.

[22] Ibid., II-2.

[23] Dr. Lani Kass, "Cyberspace: A Warfighting Domain," briefing slides, Headquarters, US Air Force, Washington, DC, September 2006, slide 14.

[24] Vice Chairman of the Joint Chiefs of Staff, General James E. Cartwright, "Definition of Cyberspace Operations," action memo for Deputy Secretary of Defense, (Washington, DC: September 29, 2008).

[25] US Joint Chiefs of Staff, *Joint Communication Systems*, Joint Publication 6-0, (Washington, DC: US Joint Chiefs of Staff, 20 March 2006), GL-11.

[26] Ibid., II-1.

[27] US Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, (Washington, DC: US Joint Chiefs of Staff, 12 April 2001, as Amended Through 13 June 2007), 111.

[28] US Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Washington, DC: US Joint Chiefs of Staff, 13 February 2006), GL-6.

[29] Ibid.

[30] Ibid., GL-5.

[31] (U) Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, (Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006) GL-1. An Unclassified, Publically Accessible, Redacted Copy of the NMS-CO, accessed at http://www.carlisle.army.mil/DIME/documents/National%20Military%20Strategy%20for%20Cyberspace%20Operations.pdf

[32] US Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, GL-5.

[33] Chairman of the Joint Chiefs of Staff, *Information Assurance (IA and Computer Network Defense (CND),* Chairman of the Joint Chiefs of Staff Instruction 6510.01, (Washington, DC: Chairman of the Joint Chiefs of Staff, 15 August 2007), GL-7.

[34] Mr. John Mense, Basic Computer Network Operations Planners Course (BCNOPC) Manager, Army 1st Information Operations Command (LAND), interview by author, Ft Belvoir, VA, 24 May 2010.

[35] George W. Bush, *The National Security Strategy of the United States of America*, (Washington, DC: The White House, March 2006), 43.

[36] Ibid., 43-44.

[37] George W. Bush, *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003), v.

[38] Catherine A. Theohary and John Rollins, *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*, CRS Report for Congress(Washington, DC: Congressional Research Service, 30 September 30, 2009), 4. (accessed at http://www.crs.gov)

[39] Executive Office of the President, *Cyberspace Policy Review*, (Washington, DC: The White House, May 2009), Executive Summary. (accessed at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA501541&Location=U2&doc=GetTRDoc.pdf).

[40] DefenseLink-Unified Command Plan Homepage, accessed at http://www.defense.gov/specials/unifiedcommand/ on 1 May 2010.

[41] USSTRATCOM Homepage, accessed at http://www.stratcom.mil/mission/ on 1 May 2010.

[42] (U) Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, 10. Reference from the unclassified, redacted version.

[43] Ibid., 11.

[44] Ibid., F-3.

[45] Ibid., F-1.

[46] Ibid., 11.

[47] Joint Electronic Library Webpage, *Joint Doctrine Hierarchy*, accessed at http://www.dtic.mil/doctrine/doctrine/status.pdf on 3 May 2010.

[48] Joint Chiefs of Staff, *Joint Communication Systems*, Joint Publication 6-0, XIII.

[49] Ibid., I-11.

[50] US Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, IX.

[51] "Dual-hatted," in this instance, means that the same officer commands both JFCC-NW and NSA.

[52] US Department of Defense, "Petraeus Cites Need for Critical Warfighting Specialties," Defense and Security News, 28 September 2009, accessed at http://www.defencetalk.com/critical-warfighting-specialties-22207/ on 20 May 2010.

[53] Ellen Nakashima, "Cyber Warfare: Challenges of the Unknown," Washington Post, 19 March 2010, accessed at http://www.cbsnews.com/stories/2010/03/19/politics/washingtonpost/main6313925.shtml on 20 May 2010.

[54] (U//FOUO) US Department of the Army, *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, Director ARCIC Approval Draft, Version 0.9*, Training and Doctrine Command Pamphlet 525-7-8 (Fort Monroe, VA: Training and Doctrine Command, 4 November 2009).

[55] Major M. Bodine Birdwell, USAF, *If You Don't Know Where You are Going, You Probably Will End Up Somewhere Else: Computer Network Operations Force Presentation,* Graduate Research Project, (Wright Patterson Air Force Base, OH: Air Force Institute of Technology, June 2009), 37.

[56] Eneken Tikk et al, *Cyber Attacks against Georgia: Legal Lessons Learned*, (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, November 2008), 4-5. This is an excellent case study of the cyber attacks against the country of Georgia that coincided with a Russian ground force operation.